

(4)

35.C14352

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

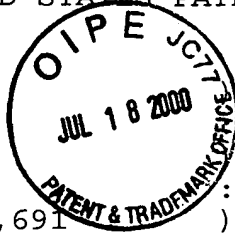
In re Application of:

MASAHIKO YAMAGUCHI

Application No.: 09/527,691

Filed: March 17, 2000

For: DATA PROCESSING APPARATUS)
AND METHOD FOR ENCRYPTION OR:)
DECRYPTION OF COMMUNICATION)
DATA :



Examiner: Not Assigned

Group Art Unit: 2787

July 18, 2000

Box Missing Parts
Commissioner for Patents
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

Applicant hereby claims priority under the International Convention and all rights to which he is entitled under 35 U.S.C. § 119 based upon the following Japanese Priority Application:

JAPAN

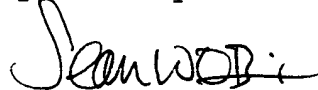
11-076758

March 19, 1999.

A certified copy of the priority document is enclosed.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our address given below.

Respectfully submitted,



Attorney for Applicant

Registration No. 37689

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

BLK\SWO\cmv

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

CF0 1435205
09/527, 691 /w
Masahiko Yamaguchi
3/14/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application

JUL 18 2000

1999年 3月19日

出願番号

Application Number:

平成11年特許願第076758号

出願人

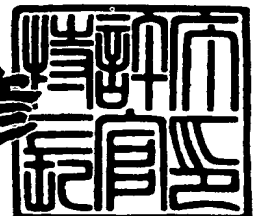
Applicant(s):

キヤノン株式会社

2000年 4月 7日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特2000-3024927

【書類名】 特許願

【整理番号】 3810009

【提出日】 平成11年 3月19日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 3/00

【発明の名称】 情報処理装置

【請求項の数】 8

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

【氏名】 山口 雅彦

【特許出願人】

【識別番号】 000001007

【氏名又は名称】 キヤノン株式会社

【代理人】

【識別番号】 100077481

【弁理士】

【氏名又は名称】 谷 義一

【選任した代理人】

【識別番号】 100088915

【弁理士】

【氏名又は名称】 阿部 和夫

【手数料の表示】

【予納台帳番号】 013424

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9703598

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置

【特許請求の範囲】

【請求項 1】 暗号化通信機能を有する情報処理装置において、
被暗号化データを入力する入力手段と、
該入力手段により入力された被暗号化データから予め定めた部分を抽出する抽出手段と、
該抽出手段により抽出された部分を暗号化する暗号化手段と、
該暗号化手段により暗号化された部分と暗号化されない部分とを合成する合成手段と、
該合成手段により合成されたデータを出力する出力手段と
を有することを特徴とする情報処理装置。

【請求項 2】 暗号化通信機能を有する情報処理装置において、
暗号化されたデータを入力する入力手段と、
該入力手段により入力されたデータから暗号化された部分を抽出する抽出手段と、
該抽出手段により抽出された暗号を解読する解読手段と、
該解読手段により解読された部分と暗号化されていない部分とを合成する合成手段と、
該合成手段により合成されたデータを出力する出力手段と
を有することを特徴とする情報処理装置。

【請求項 3】 請求項 1 において、前記被暗号化データは、印刷用データであることを特徴とする情報処理装置。

【請求項 4】 請求項 3 において、前記抽出手段は、印刷用データの中からプリンタの動作モード設定に関わる部分を抽出することを特徴とする情報処理装置。

【請求項 5】 請求項 3 において、前記抽出手段は、印刷データの中から画像データの圧縮方式の指定に関わる部分を抽出することを特徴とする情報処理装置。

【請求項 6】 請求項 1 において、前記被暗号化データは画像データであり

前記抽出手段は画像データの重み付けの大きな部分を抽出することを特徴とする情報処理装置。

【請求項 7】 請求項 1 において、前記被暗号化データは音声データであり

前記抽出手段は音声データの重み付けの大きな部分を抽出することを特徴とする情報処理装置。

【請求項 8】 請求項 1 において、前記被暗号化データは圧縮されるデータであり、

前記抽出手段は変換テーブルを抽出することを特徴とする情報処理装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、暗号化機能を有する情報処理装置に関する。

【0 0 0 2】

【従来の技術】

情報機器がネットワークに接続されるようになって、データの漏洩、盗聴などに対処する必要があるが、この対処方法として、データを暗号化する方法が有効である。

【0 0 0 3】

【発明が解決しようとする課題】

しかし、暗号が複雑になるほど暗号化処理に時間が掛かかるという問題点がある。例えば、パソコン暗号化処理した印字データをネットワーク経由でプリンタに送り、さらに、プリンタで復元化処理して印刷する際、暗号化処理のために印字速度が低下してしまう等の問題が発生していた。

【0 0 0 4】

本発明の目的は、上記のような問題点を解決し、全体の暗号化処理に掛かる時

間を短縮することができる情報処理装置を提供することにある。

【0005】

【課題を解決するための手段】

請求項1の発明は、暗号化通信機能を有する情報処理装置において、被暗号化データを入力する入力手段と、該入力手段により入力された被暗号化データから予め定めた部分を抽出する抽出手段と、該抽出手段により抽出された部分を暗号化する暗号化手段と、該暗号化手段により暗号化された部分と暗号化されない部分とを合成する合成手段と、該合成手段により合成されたデータを出力する出力手段とを有することを特徴とする。

【0006】

請求項2の発明は、暗号化通信機能を有する情報処理装置において、暗号化されたデータを入力する入力手段と、該入力手段により入力されたデータから暗号化された部分を抽出する抽出手段と、該抽出手段により抽出された暗号を解読する解読手段と、該解読手段により解読された部分と暗号化されていない部分とを合成する合成手段と、該合成手段により合成されたデータを出力する出力手段とを有することを特徴とする。

【0007】

請求項1において、被暗号化データは、印刷用データとすることができる。

【0008】

請求項3において、抽出手段は、印刷用データの中からプリンタの動作モード設定に関わる部分を抽出することができる。

【0009】

請求項3において、抽出手段は、印刷データの中から画像データの圧縮方式の指定に関わる部分を抽出することができる。

【0010】

請求項1において、被暗号化データは画像データとすることができ、抽出手段は画像データの重み付けの大きな部分を抽出することができる。

【0011】

請求項1において、被暗号化データは音声データとすることができ、抽出手段

は音声データの重み付けの大きな部分を抽出することができる。

【 0 0 1 2 】

請求項 1 において、被暗号化データは圧縮されるデータとすることができ、抽出手段は変換テーブルを抽出することができる。

【 0 0 1 3 】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して詳細に説明する。

【 0 0 1 4 】

<第 1 の実施の形態>

図 1 および図 3 は本発明の第 1 の実施の形態を示す。本実施の形態は、プリンタが送る印字データを暗号化する例である。この例では、プリンタの基本動作を決定する制御コードのみを暗号化する。制御コードはその後に続くデータの解釈の仕方を決定する重要なコードである。このため、この部分を暗号化することにより、その後に続くデータの解釈方法が不明となり、たとえデータが暗号化されていなくても、大きな暗号化効果が期待できる。

【 0 0 1 5 】

図 1 を参照して暗号化する側の構成を説明する。図 1 において、1 は印字データ入力部であり、印字データを入力するものである。2 は入力バッファであり、印字データを一時的に蓄えるものである。3 はデータ解析／抽出部であり、入力バッファ 2 に蓄えられたデータの内容を解析し、暗号化すべき部分を抽出するものである。4 は暗号化部であり、データ解析／抽出部 3 により抽出された部分を暗号化するものである。5 は出力バッファであり、送信すべきデータを一時的に蓄えるためのものである。6 は送信部であり、出力バッファ 5 のデータを送信するものである。

【 0 0 1 6 】

図 2 を参照して復元化する側の構成を説明する。図 2 において、2 1 は受信部であり、被暗号化データを受信するものである。2 2 は入力バッファであり、受信部 2 1 により受信された被暗号化データを一時的に蓄えるためのものである。2 3 は抽出部であり、入力バッファ 2 2 に蓄えられたデータの中から暗号化され

た箇所を判別して抽出するものである。24は復元化部であり、抽出部23により抽出されたデータを復元化するものである。25は出力バッファであり、印字すべきデータを一時的に蓄えるためのものである。26は出力部であり、出力バッファ25に蓄えられているデータを出力するものである。

【0017】

図3は暗号化する側の動作フローの一例を示すフローチャートである。印字データ入力部1により入力された印字データは一度入力バッファ2に蓄えられ（S301）、パターンマッチング等の判定方法によりデータ解析／抽出部3によりデータの内容が解析される（S302）。このデータの解析結果に基づき、プリンタの制御コードか否かが判別される（S303）。データ解析／抽出部3によりプリンタの制御コードとみなされた部分は暗号化部4により暗号化処理され（S304）、出力バッファ5に送られる（S305）。一方、プリンタの制御コード以外の部分は暗号化処理をされずにそのまま出力バッファ5に送られる（S306）。その後、出力バッファ5の内容は送信部6によって送信される（S307）。

【0018】

図4は復元化する側の動作フローの一例を示すフローチャートである。受信部21により受信された被暗号化データは一度入力バッファ22に蓄えられ（S401）、入力バッファ22の被暗号化データの内容が解析され（S402）、このデータの解析結果に基づき、暗号化された部分か否かが抽出部23により判別される（S403）。暗号化された部分は抽出部23により抽出され、抽出された暗号化部分は復元化処理部24による復元化処理によって復元され（S404）、出力バッファ25に送られる（S405）。一方、暗号化されていない部分は復元化処理をされずにそのまま出力バッファ25に送られる（S406）。その後、出力バッファ25の内容は出力部26により印字装置等に出力され、印字される。

【0019】

本実施の形態では、被暗号化データの全てを暗号化するのではなく、被暗号化データの重要度度の高い部分のみを暗号化することにより、全体の暗号化処理に

掛かる時間を短縮することができる。

【0020】

＜第2の実施の形態＞

図5は本発明の第2の実施の形態を示す。これは、画像データを暗号化する例であり、画像情報を表現する上で重み付けの大きな部分のみを暗号化する例である。図5において、61は画像データ入力部であり、画像データを入力するものである。62は入力バッファであり、画像データを一時的に蓄えるものである。63はデータ抽出部であり、入力バッファ62に蓄えられたデータから各RGBの上位4bit抽出するものである。64は暗号化部であり、データ抽出部63により抽出された部分を暗号化するものである。65は出力バッファであり、送信すべきデータを一時的に蓄えるためのものである。66は送信部であり、出力バッファ65のデータを送信するものである。

【0021】

次に、図6を参照して画像データの構成を説明する。画像データの各1ピクセルは3原色であるRGBが各8bitで表現され、1ピクセルあたり24bitで構成されている。画像情報を表現する上で重み付けの大きな部分は上位ビットである。例えば、RGB各8bitのうち上位4bitのデータが失われると、正しい画像情報の復元はほぼ不可能となるため、上位4bitのみを暗号化すれば、画像データ全体を暗号化しなくても大きな暗号化効果が期待できる。

【0022】

図7は本実施の形態における動作フローの一例を示すフローチャートである。画像データ入力部61により入力された画像データは、一度、入力バッファ62に蓄えられ（S701）、その後、抽出部63によりデータが解析され（S702）、RGB各データの上位4bitのみが抽出部63により抽出されると（S703）、上位4bitが暗号化部64により暗号化されて（S704）出力バッファ65に送られる（S705）。残る下位4ビットのデータは暗号化されずにそのまま出力バッファ65に送られる（S706）。その後、出力バッファ65の内容は送信部66によって送信される（S707）。

【0023】

＜第3の実施の形態＞

図8は本発明の第3の実施の形態を示す。これは音声データを暗号化する例である。図8において、91は音声データ入力部であり、音声データを入力するものである。92は入力バッファであり、音声データ入力部91により入力された音声データを一時的に蓄えるためのものである。93は抽出部であり、入力バッファ92に蓄えられたデータからビット15と、ビット11と、ビット7と、ビット3の計4bitを抽出するものである。94は暗号化部であり、抽出部93により抽出された部分を暗号化するものである。95は出力バッファであり、送信すべきデータを一時的に蓄えるためのものである。96は送信部であり、出力バッファ95のデータを送信するものである。

【0024】

図9を参照して音声データの構成を説明する。ここでの音声データはPCM方式での1つのサンプリングデータであって16bit（図9（c））で構成されている。音声情報を表現する上で重み付けの大きな部分は上位ビットであることから、基本的には上位ビットのみを暗号化すれば正しい音声情報の復元はほぼ不可能となる。しかし、録音レベルが小さい音声データでは上位ビットが使用されず0になる確率が高くなることから、第三者が盗用した際に暗号化されて不明なビットを0にマスクするという処理を行うと、録音レベルの小さな音声では容易に復元されてしまう可能性があり得る。これを防ぐため本実施の形態では、例えば、図9（a）に示すような音声波形を、図9（b）に示すように、全16bitのうち間隔をあけてビット15と、ビット11と、ビット7と、ビット3の計4bitを取り出して暗号化を行う方法をとっている。

【0025】

図10は本実施の形態における動作フローの一例を示すフローチャートである。音声データ入力部91により入力された音声データは、一度、入力バッファ92に蓄えられ（S1001）、その後、抽出部93によりデータが解析され（S1002）、ビット15と、ビット11と、ビット7と、ビット3の計4bitが抽出部93により抽出されると（S1003）、暗号化部94により暗号化さ

れ (S1004)、出力バッファ95に送られる (S1005)。残る12bitのデータは暗号化されずにそのまま出力バッファ95に送られる (S1006)。その後、出力バッファ95の内容は送信部96によって送信される (S1007)。

【0026】

<第4の実施の形態>

図11は本発明の第4の実施の形態を示す。これは圧縮されたデータを暗号化する例である。汎用的なデータ圧縮方法の1つとして、データ内に現れるパターンの分布を解析し、使用頻度の高いパターンから順に少ないビット数に割り当てるハフマン符号などを用いたテーブルを作成し、このテーブルを用いてデータ変換／圧縮を行う方法が従来より知られている。圧縮されたデータを復元するには、同じ変換テーブルを使用して元のデータに復元する。本実施の形態は、データを圧縮しながら変換テーブル部分のみを暗号化することにより、盗用された際の復元を困難にし、データ全体を暗号化するのと同等の効果を実現した例である。

【0027】

図11において、111はデータ入力部であり、データを入力するものである。112は入力バッファであり、データ入力部111により入力されたデータを一時的に蓄えるためのものである。113はデータ分布解析部であり、入力バッファ112に蓄えられたデータ中で使用されてパターンの分布を解析するものである。114は変換テーブル作成部であり、データ分布解析113の解析結果から圧縮用の変換テーブルを作成するものである。115はデータ変換／圧縮部であり、変換テーブル作成部114により作成された変換テーブルを用いて入力データを圧縮するものである。116は変換テーブル暗号化部であり、変換テーブル作成部114により作成された変換テーブルを暗号化するものである。117は出力バッファであり、データ変換／圧縮部115により得られたデータか、変換テーブル暗号化部116により得られたテーブルを蓄えるためのものである。118は送信部であり、出力バッファ117の内容を送信するものである。

【0028】

図12は本実施の形態における動作フローの一例を示すフローチャートである。データ入力部111により入力されたデータは、一度、入力バッファ112に蓄えられ（S1201）、その後、データ中に現れるパターンの分布解析がデータ分布解析部113により行われ（S1202）、この解析結果に基づき、変換テーブル作成部114により圧縮用の変換テーブルが作成される（S1203）。この変換テーブルは変換テーブル暗号化部116により暗号化され（S1204）、出力バッファ117に送り込まれる（S1205）。一方、データ変換／圧縮部115により変換テーブルを用いて入力データを圧縮し（S1206）、圧縮化されたデータは暗号化されずに出力バッファ117に送り込まれる（S1207）。そして、出力バッファ117の全データの処理が完了すると（S1208）、出力バッファ117の内容は送信部118によって送信される（S1209）。

【0029】

【発明の効果】

以上説明したように、本発明によれば、被暗号化データの全てを暗号化するのではなく、被暗号化データの重要度の高い部分のみを暗号化するようにしたので、全体の暗号化処理に掛かる時間を短縮することができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態を示すブロック図である。

【図2】

本発明の第1の実施の形態を示すブロック図である。

【図3】

暗号化する側の動作フローの一例を示すフローチャートである。

【図4】

復元化する側の動作フローの一例を示すフローチャートである。

【図5】

本発明の第2の実施の形態を示すブロック図である。

【図 6】

第 2 の実施の形態における画像データの構成を説明するための説明図である。

【図 7】

第 2 の実施の形態における動作フローの一例を示すフローチャートである。

【図 8】

本発明の第 3 の実施の形態を示すブロック図である。

【図 9】

第 3 の実施の形態における音声データの構成を説明するための説明図である。

【図 1 0】

第 3 の実施の形態における動作フローの一例を示すフローチャートである。

【図 1 1】

本発明の第 4 の実施の形態を示すブロック図である。

【図 1 2】

第 4 の実施の形態における動作フローの一例を示すフローチャートである。

【符号の説明】

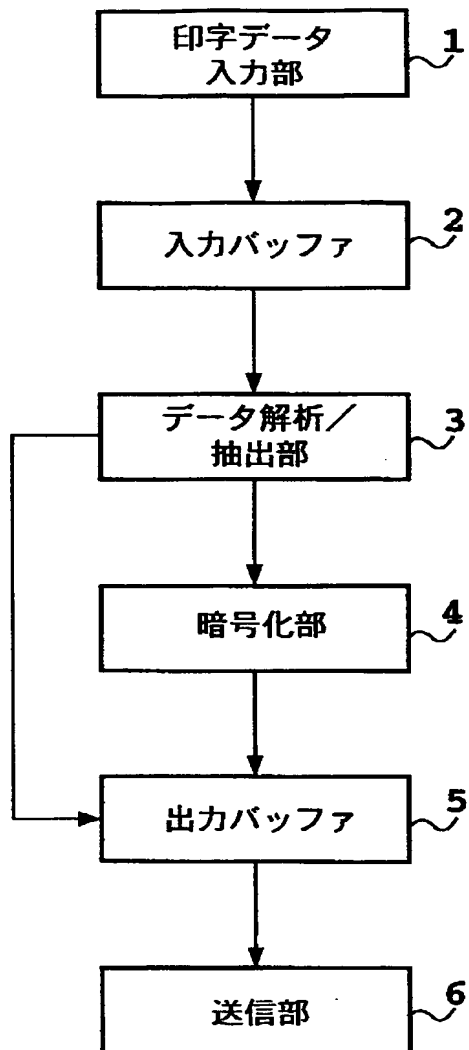
- 1 印字データ入力部
- 2, 6 2, 9 2, 1 1 2 入力バッファ
- 3 データ解析／抽出部
- 4, 6 4 暗号化部
- 5, 6 5, 9 5, 1 1 7 出力バッファ
- 6, 6 6, 9 6, 1 1 8 送信部
- 6 1 画像データ入力部
- 6 3 データ抽出部
- 9 1 音声データ入力部
- 9 3 抽出部
- 9 4 暗号化部
- 1 1 1 データ入力部
- 1 1 3 データ分布解析部
- 1 1 4 変換テーブル作成部

115 データ変換／圧縮部

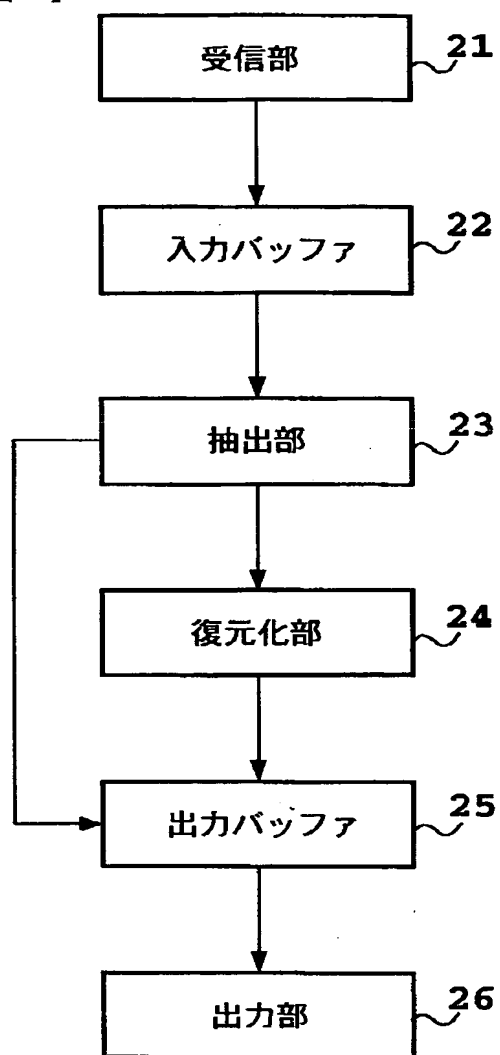
116 変換テーブル暗号化部

【書類名】 図面

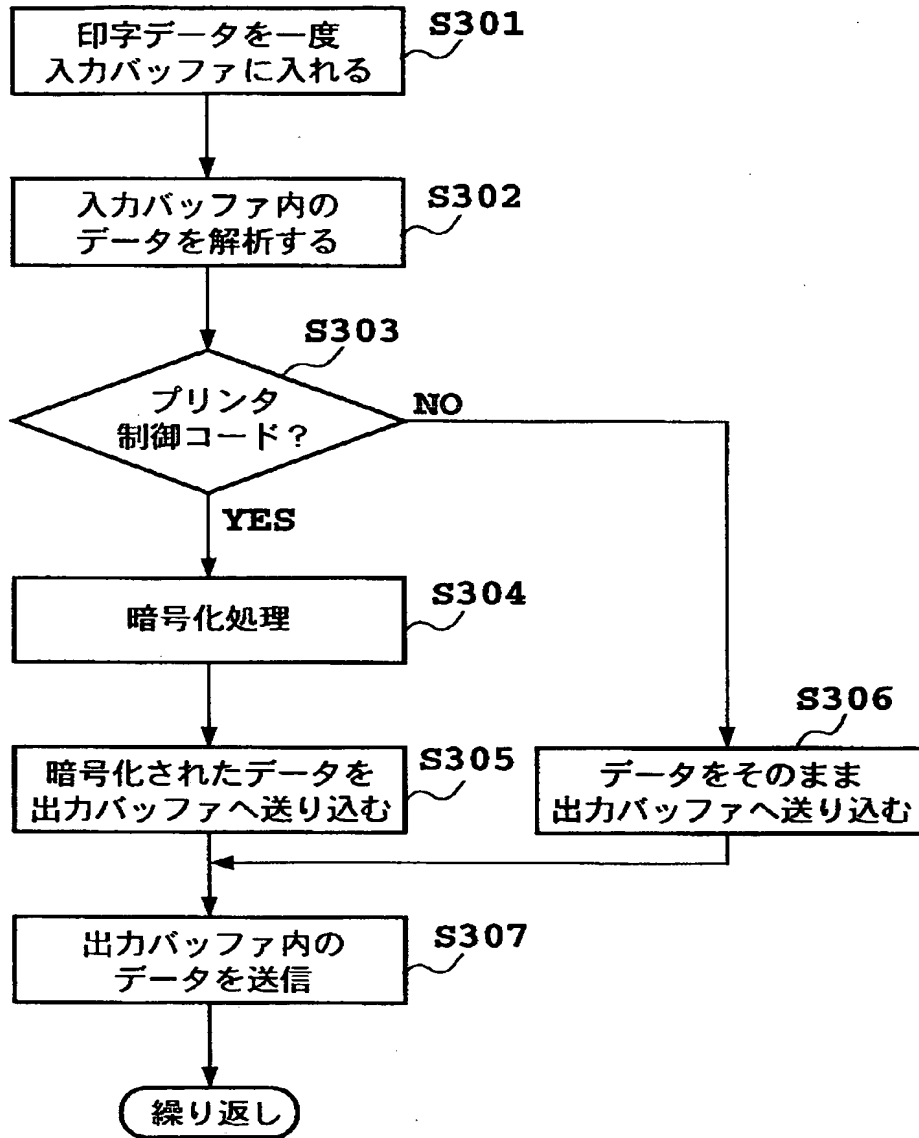
【図 1】



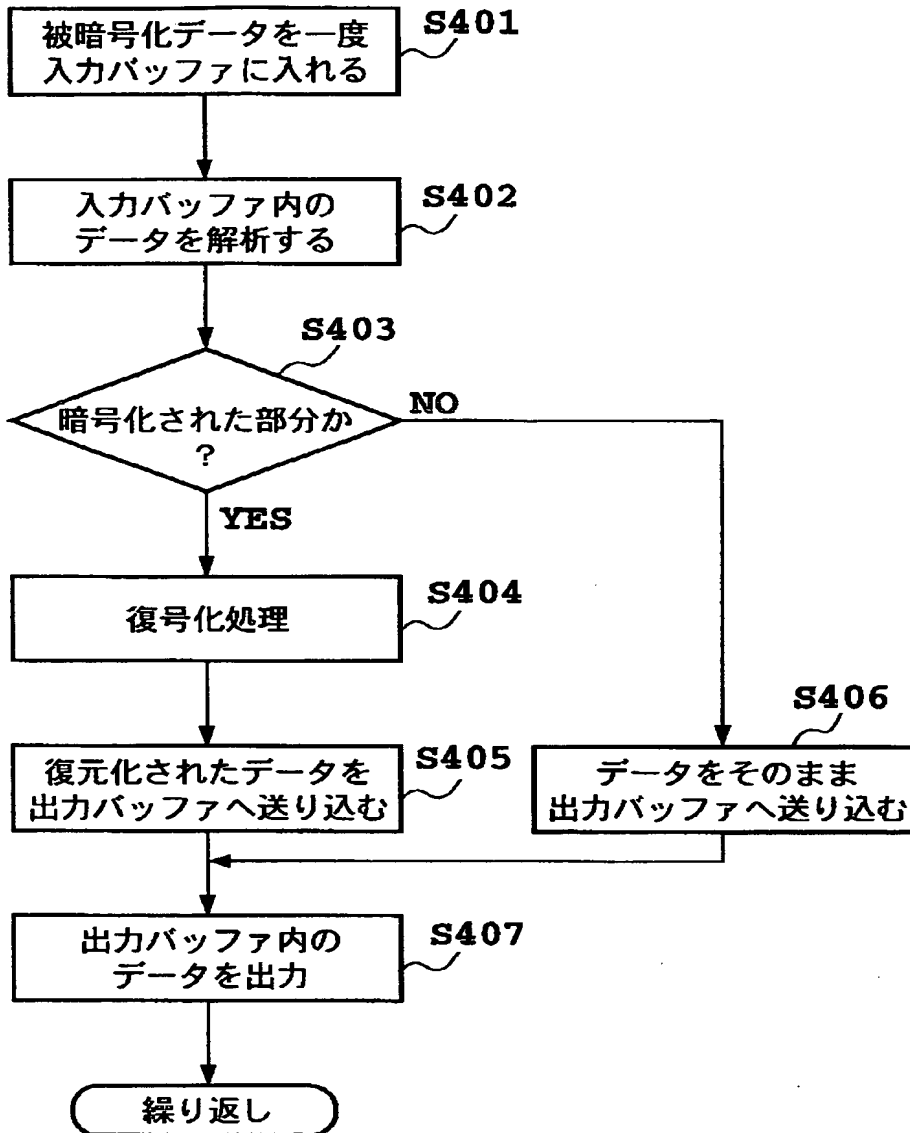
【図 2】



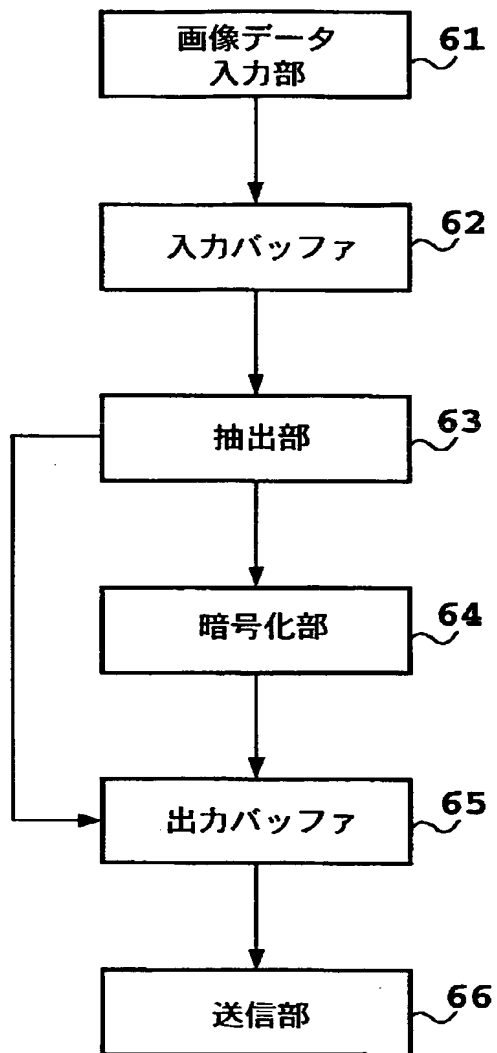
【図 3】



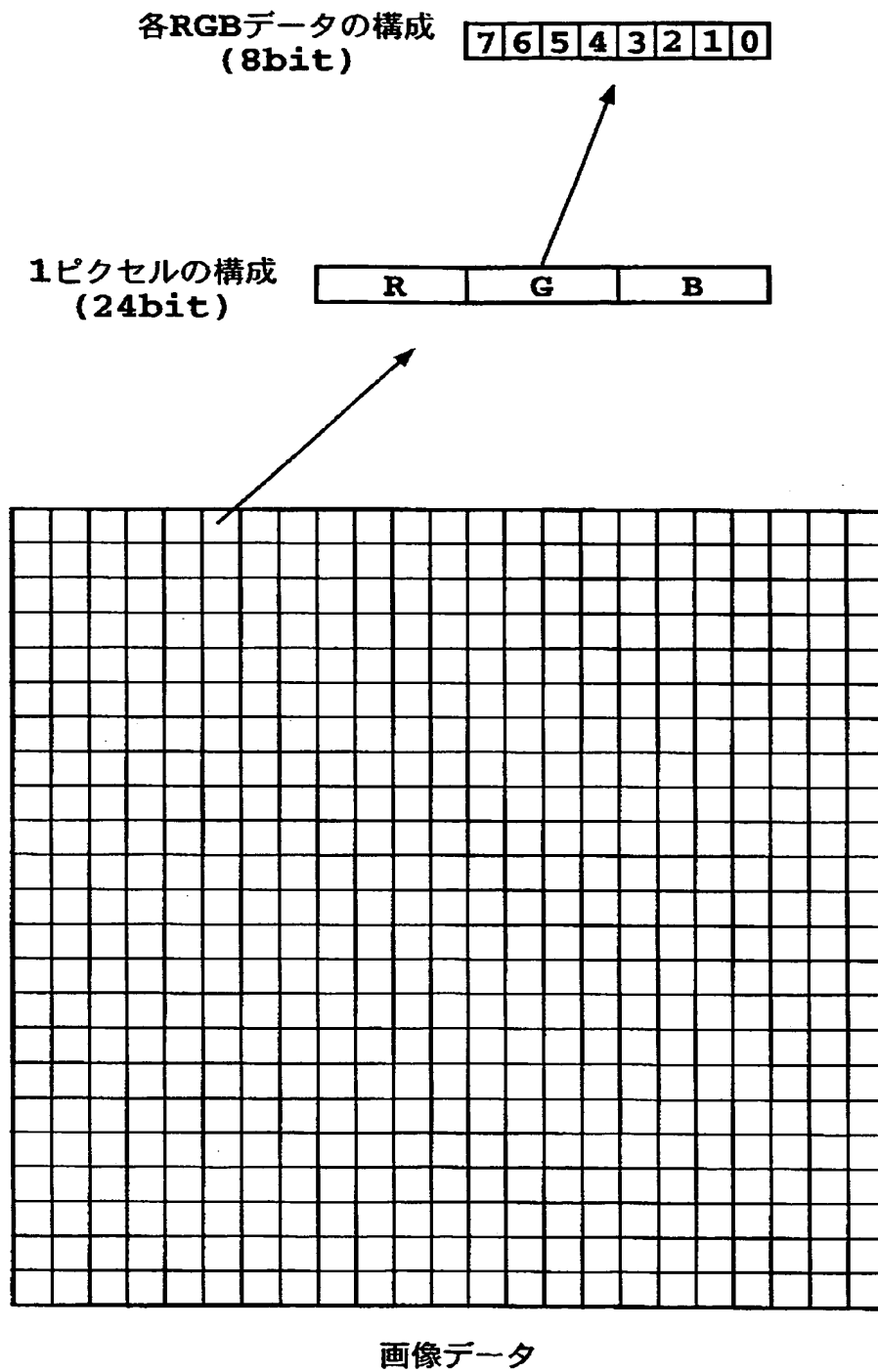
【図 4】



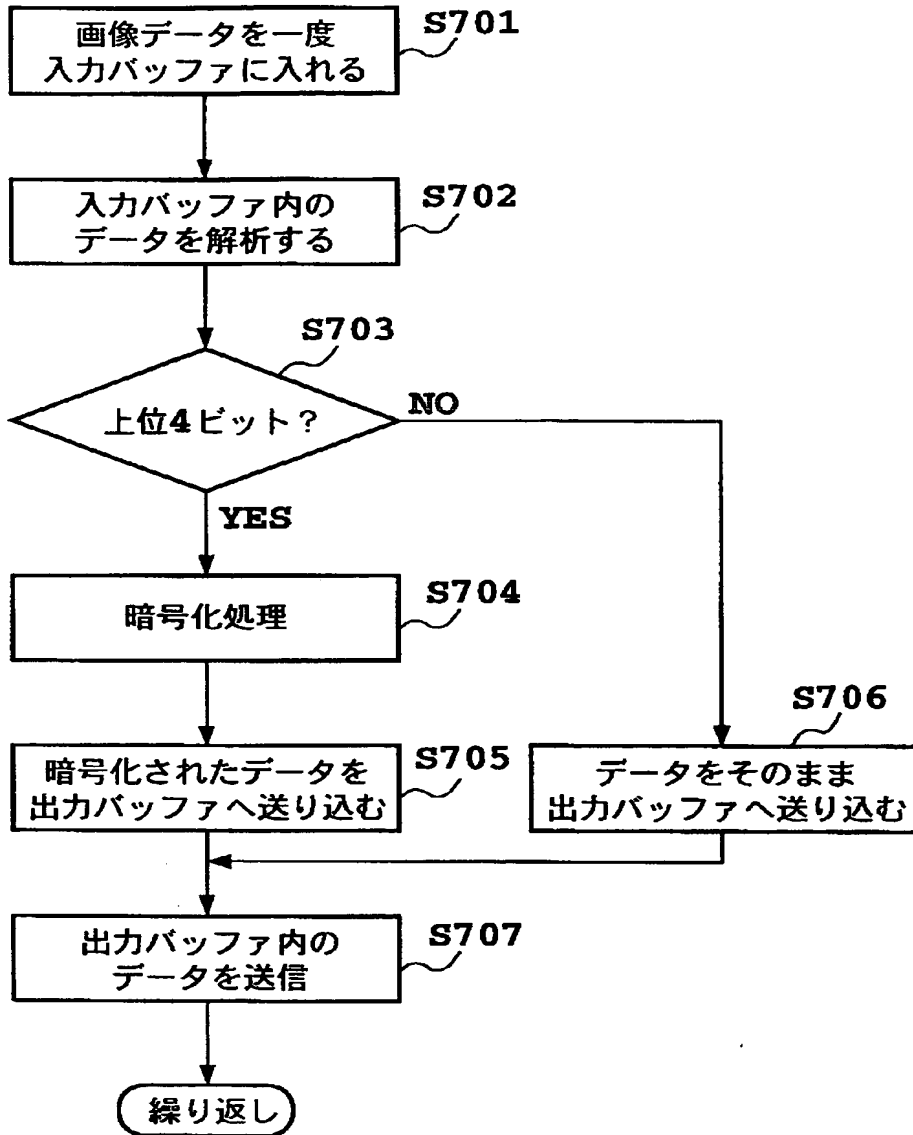
【図 5】



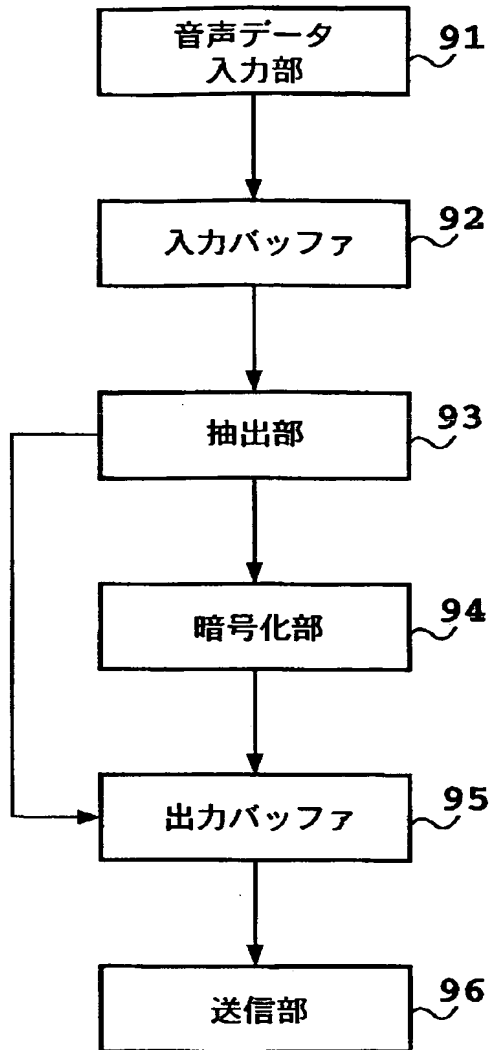
【図6】



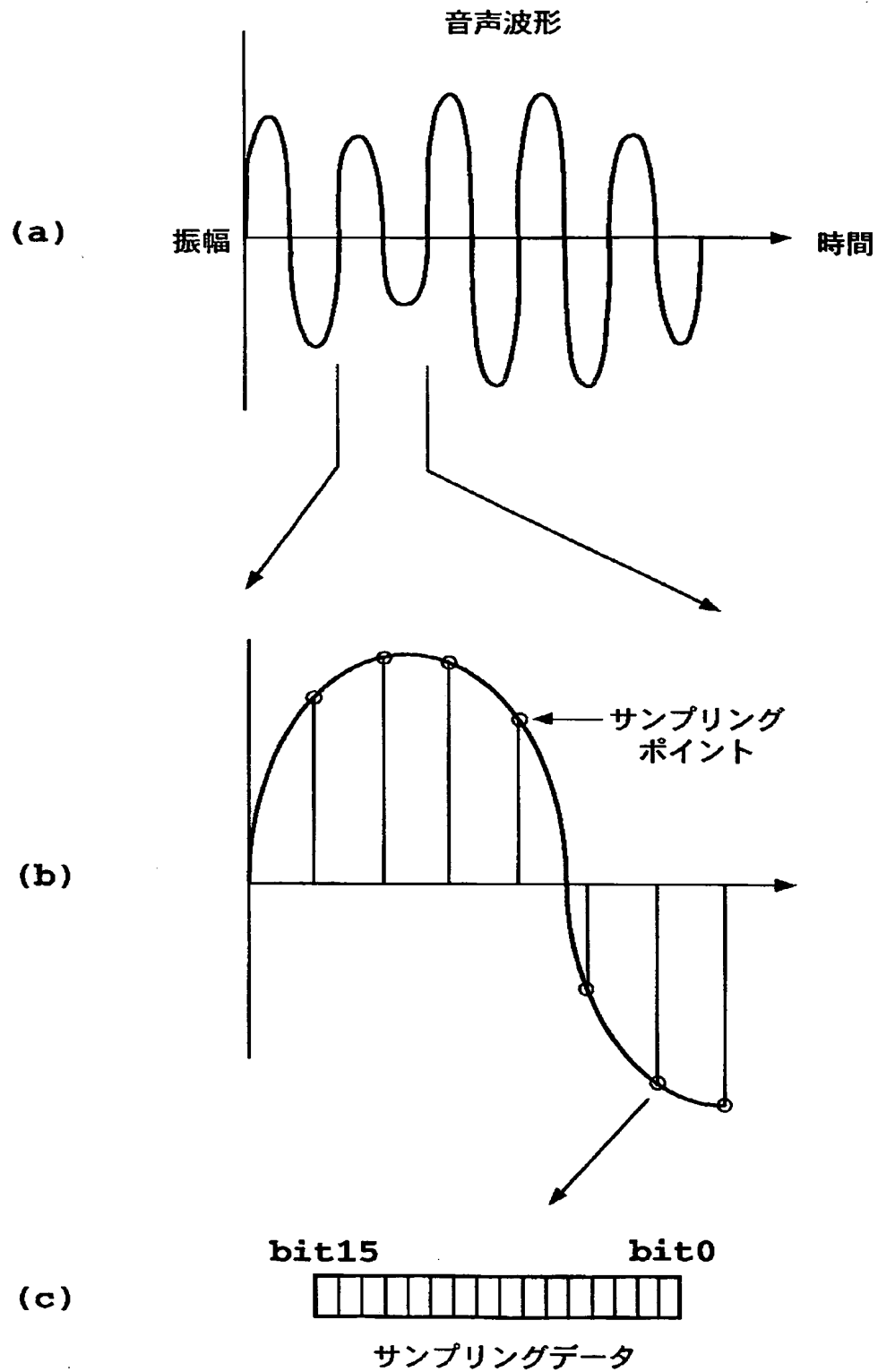
【図 7】



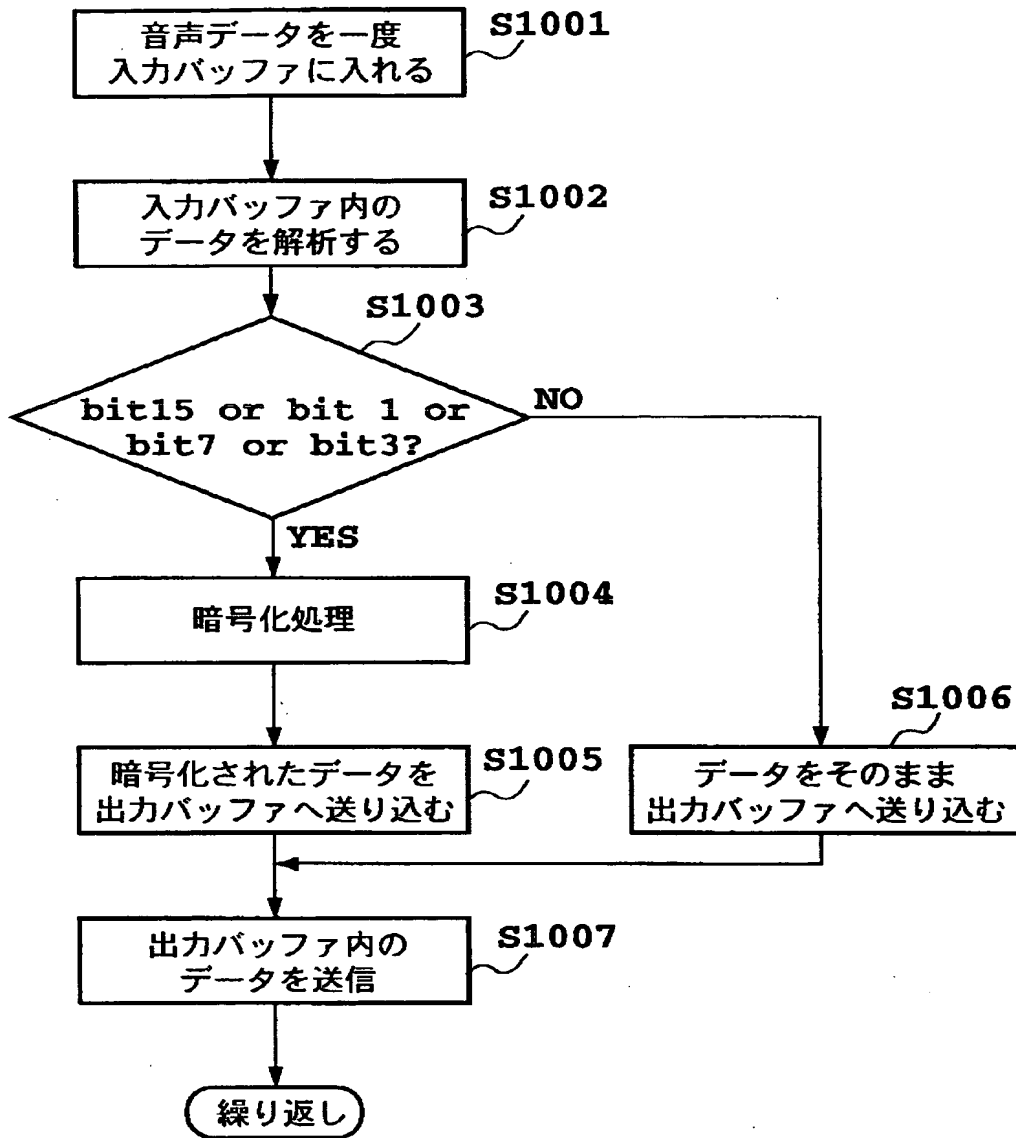
【図 8】



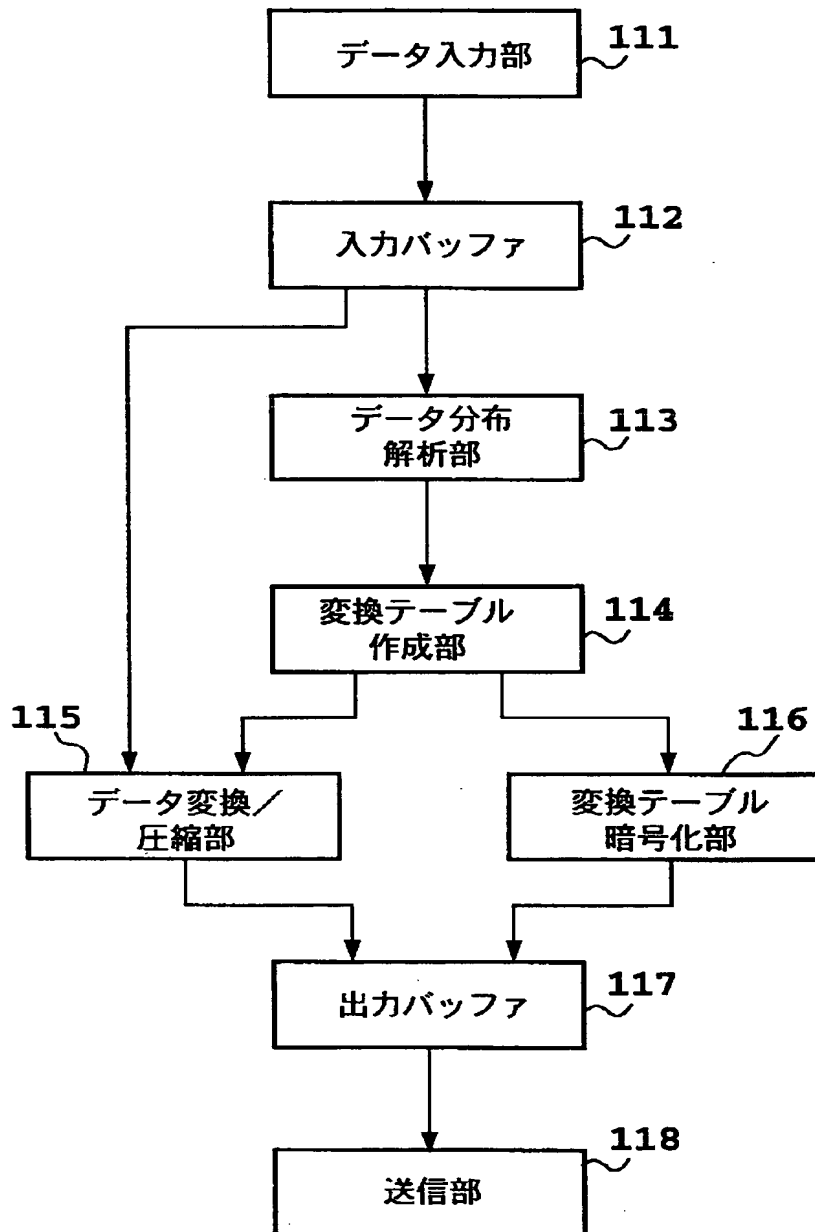
【図 9】



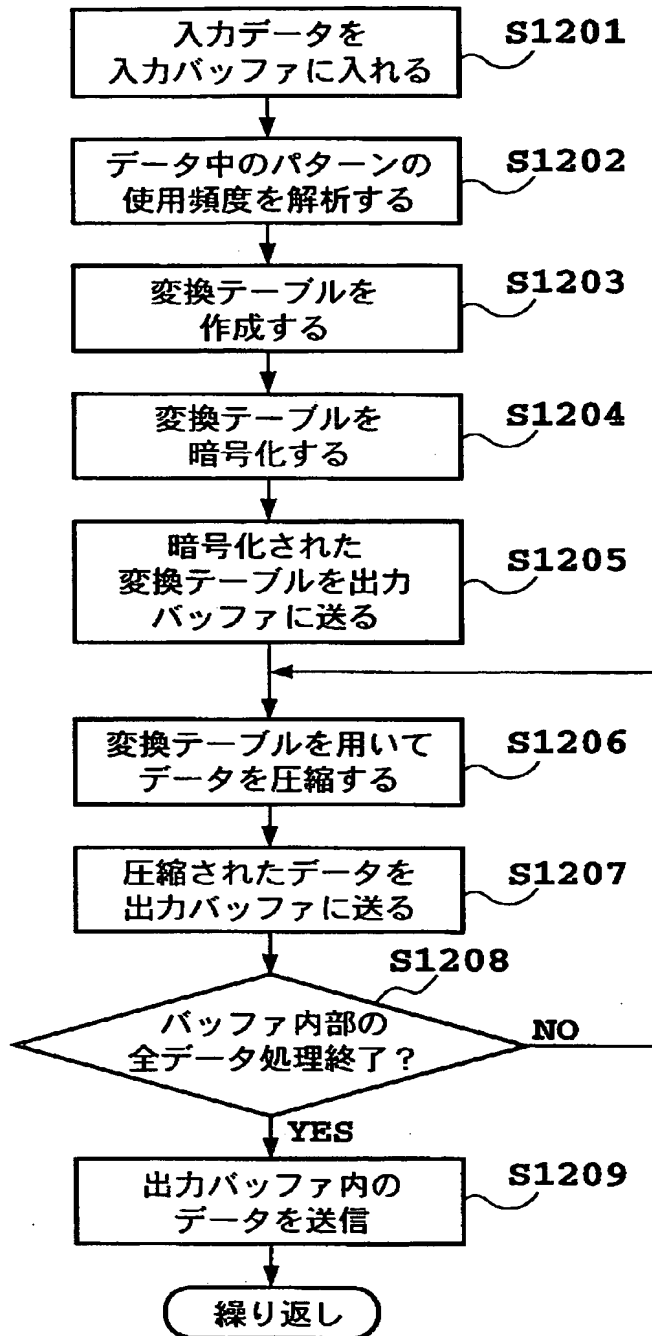
【図 10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 全体の暗号化処理に掛かる時間を短縮する。

【解決手段】 印字データ入力部 1 により入力された印字データは一度入力バッファ 2 に蓄えられ、パターンマッチング等の判定方法によりデータ解析／抽出部 3 によりデータの内容が解析される。このデータの解析結果に基づき、プリンタの制御コードか否かが判別される。データ解析／抽出部 3 によりプリンタの制御コードとみなされた部分は暗号化部 4 により暗号化処理され、出力バッファ 5 に送られる。一方、プリンタの制御コード以外の部分は暗号化処理をされずにそのまま出力バッファ 5 に送られる。その後、出力バッファ 5 の内容は送信部 6 によって送信される。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都大田区下丸子3丁目30番2号

氏 名 キヤノン株式会社